On Codes and Projective Designs (有限群論)

AUTHOR(S):

HERING, CHRISTOPH

CITATION:

HERING, CHRISTOPH. On Codes and Projective Designs (有限群論). 数理解析研究所講究録 1979, 344: 26-60

ISSUE DATE:

1979-02

URL:

http://hdl.handle.net/2433/104315

数理解析研究所講究録
344 巻 1979 年 26-60

26

On codes and projective designs

by

Christoph Hering

§ 0. Introduction

The original purpose of this paper was to investigate if the ideas of coding theory can be used to obtain information about collineation groups of incidence structures. It turns out that this is indeed the case, certainly where finite projective designs are concerned. We very easily obtain a substantial amount of information about automorphisms of these geometries. Surprisingly, some of the results we obtain are similar to the results which Hughes (1957) obtained with the help of the Hasse-Minkowski Theorem on the rational equivalence of quadratic forms. The new methods however seem in principal to be more general, and they can be more readily adapted to specific situations. On the other hand, they are only really powerful if there exists a prime dividing the order of the given design to the first power.

In § 3 we present a description of the codes over GF(2) arising from projective planes of finite even order. This is not necessary for our investigation of collineation groups. It might, however, help to obtain some insight into the nature of these codes. Also it leads to an existence proof for the "large" Mathieu groups which is somewhat shorter than the one presented in Lüneburg (1969). We construct here only M_{22} (see § 4).

§ 1. Codes

A code is a subset of a metric space. In this chapter we shall restrict ourselves to sets of points in Hamming spaces, where a Hamming space is a metric space defined in the following way:

1.1 Definition. Let $\mathcal{P}$ and F be non-empty sets and V the set of all functions from $\mathcal{P}$ into F. For $f,g \in V$ define

$$d(f,g) = |\{x \in \mathcal{P} \mid f(x) \neq g(x)\}|.$$

Then (V,d) is called a Hamming space.

Note that in 1.1 obviously d satisfies the triangle inequality. For $\mathcal{C} \subseteq V$ we define

$$d_m(\mathcal{C}) = \min_{\substack{f,g \in \mathcal{C} \\ \text{and } f \neq g}} d(f,g)$$

and call it the minimum distance of $\mathcal{C}$. One of the objectives of coding theory is to find codes $\mathcal{C}$ of large cardinality such that $d_m(\mathcal{C})$ is not too small.

If F is a field, then V becomes a vector space over F. For this case we define $w(f) = d(0,f)$, which is just the cardinality of the support of f. We call w(f) the weight of f. Note that now $d(f,g) = w(f-g)$ for $f,g \in V$.

A code $\mathcal{C} \subseteq V$ is linear if F is a field and $\mathcal{C}$ is a subspace of V. In a linear code $\mathcal{C}$,

$$d_m(\mathfrak{C}) = \min_{f \in \mathfrak{C} \setminus \{0\}} w(f).$$

If $\mathfrak{X}$ is a subset of $\mathfrak{P}$, then the <u>characteristic function</u> $f_{\mathfrak{X}}$ of $\mathfrak{X}$ is defined by

$$f_{\mathfrak{X}}(P) = \begin{cases} 1 & \text{if } P \in \mathfrak{X} \\ 0 & \text{if } P \notin \mathfrak{X}. \end{cases}$$

There is an obvious way for constructing codes from incidence structures: Assume that $\mathfrak{P}$ is the set of points of an incidence structure $(\mathfrak{P},\mathfrak{B},I)$, and F is a field. Let

$$\mathfrak{A} = \langle f_{(b)} \mid b \in \mathfrak{B} \rangle.$$

Then of course $\mathfrak{A}$ is a code in V. Codes constructed in this way are frequently interesting from the point of view of coding theory. Appart from that, they can be used to obtain information about the geometrical properties of $(\mathfrak{P},\mathfrak{B},I)$.

Let $\mathfrak{C}$ be a code over a field. For each non-negative integer i we define

$$\mathfrak{C}_i = \{x \in \mathfrak{C} \mid w(x) = i\}$$

and $w_i = w_i(\mathfrak{C}) = |\mathfrak{C}_i|$.

§ 2. Codes derived from finite projective planes

Let $(\mathcal{P},\mathcal{L})$ be a projective plane of finite order n and F a field. Furthermore, let V be the set of all functions from $\mathcal{P}$ into F, and let

$$\mathcal{A} = \langle f_{(\ell)} \mid \ell \in \mathcal{L} \rangle .$$

Let $\mathbb{I}$ be an incidence matrix of $(\mathcal{P},\mathcal{L})$. Note that the dimension of $\mathcal{A}$ is just the rank of $\mathbb{I}$, if we consider $\mathbb{I}$ as a matrix over F. It is quite important for our theory to obtain information about the dimension of $\mathcal{A}$. The following lemma contains a (certainly not very good) lower bound:

2.1 Lemma. Let P and Q be two different points in $\mathcal{P}$ and $\ell \in [Q] - \{PQ\}$. Then the set

$$\left\{ f_{(g)} \;\middle|\; g \in [P] \cup [Q] \setminus \{\ell\} \right\}$$

is lineary independent. In particular, $\dim \mathcal{A} \geq 2n$.

Proof. Denote $g_0 = PQ$, $\{g_1,\cdots,g_n\} = [P] - \{g_0\}$ and $\{g_{n+1},\cdots, g_{2n-1}\} = [Q] - \{g_0,\ell\}$. Let $a_0,\cdots,a_{2n-1} \in F$ and $f = \sum_{i=0}^{2n-1} a_i f_{(g_i)}$. Assume that $f = 0$. If $X \in PQ - \{P,Q\}$, then $f(X) = a_0$, so that $a_0 = 0$. Let $1 \leq i \leq n$ and $X = g_i \cap \ell$. Then $0 = f(X) = a_i$. Let $n + 1 \leq j \leq 2n - 1$ and $Z = g_j \cap g_i$ for some i between 1 and n. Then $0 = f(Z) = a_i + a_j = a_j$.

For $f \in V$ and $\mathfrak{x} \subseteq \mathcal{P}$, denote $\int_{\mathfrak{x}} f = \sum_{X \in \mathfrak{x}} f(X)$. Also, let $V_0 = \{f \in V \mid \int_{\mathcal{P}} f = 0\}$ and let E be the function in V

which maps each element of $\mathfrak{P}$ onto the identity of F. Set $\mathfrak{A}_{\ddot{o}} = V_{\ddot{o}} \cap \mathfrak{A}$.

2.2 Lemma. $V_{\ddot{o}}$ is a hyperplane of V. Furthermore, $V = \langle E \rangle \oplus V_{\ddot{o}}$, unless char $F = p < \infty$ and $p \mid n^2+n+1$, in which case $\langle E \rangle \leq V_{\ddot{o}}$.

Proof. The map

$$f \longmapsto \int_{\mathfrak{P}} f \qquad \text{for all } f \in V$$

is an epimorphism of V onto F with kernel $V_{\ddot{o}}$. Clearly $E \in V_{\ddot{o}}$ if and only if char $F \mid |\mathfrak{P}| = n^2+n+1$.

2.3 Lemma. a) $\mathfrak{A} = V$ unless F has finite characteristic p and $p \mid n(n+1)$.

b) If char $F = p < \infty$ and $p \mid n+1$, then $\mathfrak{A} = V_{\ddot{o}}$ and $V = \langle E \rangle \oplus \mathfrak{A}$.

c) If char $F = p < \infty$ and $p \mid n$, then $E \in \mathfrak{A}$ and $\mathfrak{A} = \langle E \rangle \oplus \mathfrak{A}_{\ddot{o}}$.

Proof. a) Consider the incidence matrix $\mathbf{I}$ as a matrix over F. We have $|\det \mathbf{I}| = (n+1)n^{(n^2+n)/2}$ by I.x.x. So $\det \mathbf{I} \neq 0$ and $\dim \mathfrak{A} = \operatorname{rank} \mathbf{I} = n^2+n+1$ unless F has characteristic $p < \infty$, where $p \mid n$ or $p \mid n+1$.

b) If $P \in \mathfrak{P}$, then

$$nf_{\{P\}} = \sum_{\ell \in [P]} f_{(\ell)} - E.$$

So $V = E + \mathfrak{A}$, as $p \nmid n$. Since $p \mid n+1$, each characteristic function $f_{(\ell)}$ for a line $\ell \in \mathfrak{L}$ lies in $V_{\ddot{o}}$. Therefore $\mathfrak{A} \leq V_{\ddot{o}}$.

Finally, p cannot divide both n+1 and n^2+n+1, so that $V = \langle E \rangle \oplus V_{\ddot{o}} = E \oplus \mathfrak{A}$ by Lemma 2.2.

c) Here $E \in \mathfrak{A}$, as

$$\sum_{\ell \in \Omega} f_{(\ell)} = (n+1)\, E$$

and $p \nmid n+1$. Hence $\mathfrak{A}_{\ddot{o}}$ is a hyperplane of $\mathfrak{A}$ by Lemma 2.2.

This together with the preceding lemma seems to indicate that the code $\mathfrak{A}$ for our purposes is most interesting if F has finite characteristic p and p|n. Therefore we shall in the remaining part of this paragraph restrict ourselves to this case. Then, as we shall see in Lemma 2.4, we really do get a non-trivial situation.

Let P_0 be a further point and let $\mathfrak{P}^* = \mathfrak{P} \cup \{P_0\}$. Let V^* be the space of all functions from $\mathfrak{P}^*$ into F. For $f \in V$ we define $\overline{f} \in V^*$ by $\overline{f}(X) = f(X)$ for $X \in \mathfrak{P}$ and $\overline{f}(P_0) = -\sum_{X \in \mathfrak{P}} f(X)$. Clearly $-$ defines a monomorphism from V into V^*, and $\overline{V} = (V^*)_{\ddot{0}}$. Also, we define a bilinear form on V^*:

$$(f,g) = -f(P_0)g(P_0) + \sum_{X \in \mathfrak{P}} f(X)g(X) \quad \text{for all } f,g \in V^*.$$

Clearly, this form is non-degenerate.

2.4 Lemma. If p|n, then $\overline{\mathfrak{A}} \leq \overline{\mathfrak{A}}^{\perp}$ and $\dim \mathfrak{A} \leq (n^2+n+2)/2$.

Proof. Let $\ell \neq h \in \mathfrak{L}$. We have $(\overline{f}_{(\ell)}, \overline{f}_{(\ell)}) = -(-(n+1))(-(n+1)) + n+1 = -n^2 - n = 0$ as p|n, and $(\overline{f}_{(\ell)}, \overline{f}_{(h)}) = -(n+1)^2 + 1 = -n^2 - 2n = 0$. Hence $\overline{\mathfrak{A}} \subseteq \overline{\mathfrak{A}}^{\perp}$, and $\dim \overline{\mathfrak{A}} \leq \dim \overline{\mathfrak{A}}^{\perp} \leq n^2+n+2 - \dim \overline{\mathfrak{A}}$, so that $\dim \mathfrak{A} = \dim \overline{\mathfrak{A}} \leq (n^2+n+2)/2$.

2.5 Theorem. If p$\nmid$n, then $\dim \mathfrak{A} = (n^2+n+2)/2$.

Proof. Consider the incidence matrix $\mathbb{I}$ as a matrix over the real numbers. There exists matrices M and N over $\mathbb{Z}$ of determinant 1 or -1 such that

$$\mathrm{MIN} = \begin{bmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_r \end{bmatrix}$$

where $r = n^2 + n + 1$ (see e. g. van der Waerden, 1967, Kapitel 12, § 85).

Hence $e_1 \ldots e_{n^2+n+1} = \det \mathrm{MIN} = \pm \det \mathbb{I} = \pm (n+1) n^{(n^2+n)/2}$.

As $p \nmid n+1$ and $p^2 \nmid n$, the number of e_i's divisible by p is at most $(n^2+n)/2$, so that at least $n^2+n+1 - (n^2+n)/2 = (n^2+n+2)/2$ of the e_i's is not divisible by p. Let $\hat{}$ denote the reduction modulo p. Then $\hat{M}$ and $\hat{N}$ have determinant ± 1, so that the rank of $\mathbb{I}$ considered as a matrix over F is equal to the rank of

$$\hat{\mathrm{MIN}} = \begin{bmatrix} \hat{e}_1 & & 0 \\ & \ddots & \\ 0 & & \hat{e}_r \end{bmatrix}$$

So rank $\hat{\mathbb{I}} \geq (n^2+n+2)/2$. Combining this with 2.4 we obtain our theorem.

Mac Williams, Sloane and Thompson (1973) attribute this result for p=2 to a forthcoming paper of Thompson. The fact, that it is true in general was first pointed out to me by E.F. Asmus, Jr.

2.6 Lemma. If $p \mid n$, then $V^* = \langle \bar{E}, f_{\{P_0\}} \rangle \perp \bar{V}_{\ddot{o}}$.

Proof. Clearly $\langle \bar{E}, f_{\{P_0\}} \rangle$ has dimension 2. Let $a\bar{E} + b f_{\{P_0\}} = \bar{h}$ for $a,b \in F$ and $h \in V_{\ddot{o}}$. Then

2.6

$0 = \int_{\mathfrak{P}^*} \overline{h} = b$, as $\overline{V} = (V^*)_{\ddot{o}}$. Therefore $-a = \overline{h}(P_0) = -\int_{\mathfrak{P}} h = 0$ and $\overline{h} = 0$. Comparing dimensions we see that $V^* = \langle \overline{E}, f_{\{P_0\}} \rangle \oplus \overline{V}_{\ddot{o}}$. If $v \in V_{\ddot{o}}$, then $\overline{v}(P_0) = -\int_{\mathfrak{P}} v = 0$, so that $(f_{\{P_0\}}, \overline{v}) = 0$ and $(\overline{E}, \overline{v}) = \sum_{X \in \mathfrak{P}} E(X)v(X) = \int_{\mathfrak{P}} v = 0$. This proves our lemma.

If $p|n$, then $E \in \mathfrak{a}$ by 2.3c). Let $v \in \overline{\mathfrak{a}}^{\perp}$. Then $0 = (\overline{E}, v) = -\overline{E}(P_0)v(P_0) + \int_{\mathfrak{P}} v = v(P_0) + \int_{\mathfrak{P}} v = \int_{\mathfrak{P}^*} v$. Hence $\overline{\mathfrak{a}}^{\perp} \leq (V^*)_{\ddot{o}} = \overline{V}$. We denote the preimage under $-$ of $\overline{\mathfrak{a}}^{\perp}$ in V by $\hat{\mathfrak{a}}$. Note that $\mathfrak{a} \leq \hat{\mathfrak{a}}$ by 2.4.

3.1

§ 3. The case $|F| = 2$ and $2|n$

In this section we keep the notation introduced in §2 and assume in addition that $|F| = 2$ and $2|n$. Our results generalize the work of Mac Williams, Sloane and Thompson (1973), who investigated the case $n = 10$. Since $F = \{0,1\}$, each element of V^* is the characteristic function of some subset of $\mathfrak{P}^*$, so that we can identify V^* with the power set of $\mathfrak{P}^*$. Also, we have $v + w = v \cup w \setminus v \cap w$ for $v,w \subseteq \mathfrak{P}^*$. In the same way we can identify V with the power set of $\mathfrak{P}$. Concerning the monomorphism $\bar{}$ from V into V^* we have for all $v \subseteq \mathfrak{P}$

$$\bar{v} = \begin{cases} v & \text{if } |v| \equiv 0 \pmod 2 \\ v \cup \{\mathfrak{P}_0\} & \text{if } |v| \equiv 1 \pmod 2. \end{cases}$$

So $|\bar{v}| \equiv 0 \pmod 2$ for all $v \in V$. Also, $w(v) = |v|$, the weight of an element is just its cardinality. Finally, we have a geometrical interpretation of our bilinear form on V^*:

If $x,y \subseteq \mathfrak{P}^*$, then

$$(x,y) = \begin{cases} 0 & \text{if } |x \cap y| \equiv 0 \pmod 2 \\ 1 & \text{if } |x \cap y| \equiv 1 \pmod 2. \end{cases}$$

Therefore Lemma 2.4 implies

3.1 Lemma. If $v,w \in \mathfrak{A}$, then $|\bar{v} \cap \bar{w}| \equiv 0 \pmod 2$.

3.2 Lemma. $|a| = |\bar{a}| \equiv 0 \pmod 4$ for each $a \in \mathfrak{A}_{\ddot{o}}$.

Proof. If $\mathfrak{l} \in \mathfrak{L}$, then $|E+\mathfrak{l}| = n^2 \equiv 0 \pmod 4$, so that in particular $E + \mathfrak{l} \in \mathfrak{A}_{\ddot{o}}$.

Also,

$$E + \langle E+\ell \mid \ell \in \mathfrak{L} \rangle \geq \langle \ell \mid \ell \in \mathfrak{L} \rangle = \mathfrak{A},$$

so that

$$\mathfrak{A}_{\ddot{o}} = \langle E+\ell \mid \ell \in \mathfrak{L} \rangle.$$

Hence each element $a \in \mathfrak{A}_{\ddot{o}}$ can be represented in the form $a = (E+\ell_1) + \cdots + (E+\ell_r)$, where $\ell_i \in \mathfrak{L}$ for $1 \leq i \leq r$. We prove our lemma by induction on r: Let $b,c \in \mathfrak{A}_{\ddot{o}}$ such that $|b| \equiv |c| \equiv 0 \pmod 4$. By Lemma 3.1 we have $|b \cap c| = |\overline{b} \cap \overline{c}| \equiv$ $\equiv 0 \pmod 2$, so that $|b+c| = |(b \cup c) \setminus (b \cap c)| = |b|+|c| -2|b \cap c| \equiv$ $\equiv 0 \pmod 4$.

A consequence of Lemma 3.2 is

3.3 Corollary. If $a \in \mathfrak{A} - \mathfrak{A}_{\ddot{o}}$, then $|a| \equiv n+1 \pmod 4$ and $|\overline{a}| \equiv n+2 \pmod 4$.

Proof. By 2.3c, there exists an element $a_{\ddot{o}} \in \mathfrak{A}_{\ddot{o}}$ such that $a = E + a_{\ddot{o}}$. Here $|a| = n^2+n+1 - |a_{\ddot{o}}| \equiv n+1 \pmod 4$ as $4|n^2$ and $4 \mid |a_{\ddot{o}}|$ by 3.2. In particular, $|a| \equiv 1 \pmod 2$, so that $\overline{a} = a \cup \{P_0\}$, and $|\overline{a}| \equiv n+2 \pmod 4$.

3.4 Lemma. If $a \in V$, then $a \in \hat{\mathfrak{A}}$ if and only if $|\ell \cap a| \equiv |a| \pmod 2$ for all $\ell \in \mathfrak{L}$.

Proof. Assume at first, that $a \in \hat{\mathfrak{A}}$ and let $\ell \in \mathfrak{L}$. Then $\overline{a} \in \overline{\mathfrak{A}}^{\perp}$ by the definition of $\hat{\mathfrak{A}}$. So $(\overline{a},\overline{\ell}) = 0$ and $|\overline{a} \cap \overline{\ell}| \equiv 0 \pmod 2$. Assume at first that $|a|$ is even. Then

$\overline{\ell} \cap \overline{a} = \overline{\ell} \cap a = \overline{\ell} \cap (\dot{a} \cap \mathfrak{P}) = (\overline{\ell} \cap \mathfrak{P}) \cap a = \ell \cap a$ and hence $|\ell \cap a| = |\overline{\ell} \cap \overline{a}| \equiv 0 \pmod 2$. Assume now that $|a|$ is odd. Then $\overline{\ell} \cap \overline{a} = (\ell \cap a) \cup \{P_0\}$, so that $|\ell \cap a| = |\overline{\ell} \cap \overline{a}| - 1 \equiv 1 \pmod 2$.

Assume on the other hand that $|\ell \cap a| \equiv |a| \pmod 2$ for all $\ell \in \mathfrak{L}$. The same type of argumentation shows that $\overline{a} \in \overline{\mathfrak{L}}^{\perp}$.

3.5 Lemma. If $\emptyset \neq a \in \hat{\mathfrak{L}}$, then $|a| \geq n+1$.

Proof. Assume at first that $|a|$ is odd. Clearly we can assume that a is a proper subset of $\mathfrak{P}$. Let $P \in \mathfrak{P} \setminus a$ and let $\ell \in [P]$. Then $|\ell \cap a| \equiv |a| \equiv 1 \pmod 2$ by Lemma 3.4. In particular, $\ell \cap a \neq \emptyset$, so that $|a| \geq |[P]| = n+1$. Assume now that $|a|$ is even. Choose a point $P \in a$. If $\ell \in [P]$, then $|\ell \cap a| \geq a$ by Lemma 3.4. Hence $|a| \geq n+2$.

3.6 Lemma. Let $k \in \mathbb{N}$ and $a \in \hat{\mathfrak{L}}_{n+k}$. If $\ell \in \mathfrak{L}$ and $\ell \neq a$, then $|a \cap \ell| \leq k$.

Proof. Assume at first that k is odd. If $\ell \subseteq a$, then $|\ell+a| = k-1$, so that $k \geq n+2$ by 3.5 and hence certainly $|a \cap \ell| = |\ell| \leq k$. So we can assume that there exists a point $P \in \ell \setminus a$. There are n lines in $[P]\setminus\{\ell\}$. Each of these lines intersects a in at least one point by 3.4. So $|a \setminus \ell| \geq n$ and hence $|a \cap \ell| \leq k$.

Assume now that k is even, and assume furthermore, that $a \cap \ell$ contains a point P. Then each line in $[P]\setminus\{\ell\}$ intersects $a \setminus \ell$ in at least one point, again by 3.4. So once more $|a \setminus \ell| \geq n$.

3.7 Lemma. $\hat{\mathfrak{A}}_{n+1} = \mathfrak{L}$.

Proof. By definition $\mathfrak{L} \subseteq \mathfrak{A}_{n+1} \subseteq \hat{\mathfrak{A}}_{n+1}$. Let $a \in \hat{\mathfrak{A}}_{n+1}$. Choose two different points P and Q in a. Then $a = PQ$ by 3.6.

3.8 Theorem. If n is even, then $\hat{\mathfrak{A}}_{n+2}$ is the set of hyperovals of $(\mathfrak{P},\mathfrak{L})$. Also, $\hat{\mathfrak{A}}_{n+2} \subseteq \mathfrak{A}$ if $n \equiv 2 \pmod 4$ and $\hat{\mathfrak{A}}_{n+2} \subseteq \hat{\mathfrak{A}} - \mathfrak{A}$ if $n \equiv 0 \pmod 4$.

Proof. Let $v \in \hat{\mathfrak{A}}_{n+2}$. Then each line intersects v in at most 2 points by Lemma 3.6, so that v is a hyperoval.

On the other hand, let $\mathfrak{f}$ be a hyperoval and $\mathfrak{l} \in \mathfrak{L}$. Then $|\mathfrak{f} \cap \mathfrak{l}| = 0$ or 2. Hence $|\mathfrak{f} \cap \mathfrak{l}| \equiv 0 \equiv |\mathfrak{f}| \pmod 2$ and $\mathfrak{f} \in \hat{\mathfrak{A}}$ by 3.4.

If $n \equiv 2 \pmod 4$, then $\overline{\mathfrak{A}} = \overline{\mathfrak{A}}^{\perp}$ so that $\hat{\mathfrak{A}} = \mathfrak{A}$ and hence $\hat{\mathfrak{A}}_{n+2} \subseteq \mathfrak{A}$. If $n \equiv 0 \pmod 4$, then $n+2 \equiv 2 \pmod 4$ and $\mathfrak{A}$ does not contain any vector of weight n+2 by 3.3.

3.9 Remark. By the famous Mac William identity [ ], the weight enumerator of $\overline{\mathfrak{A}}^{\perp}$ is determined by the weight enumerator of $\overline{\mathfrak{A}}$. Hence Theorem 3.8 shows that the number of hyperovals in $(\mathfrak{P},\mathfrak{L})$ can be computed from the weight enumerator of $\mathfrak{A}$.

3.10 Lemma on various vectors of small weight.
Let $v \in \hat{\mathfrak{A}}$ and define

$$\mathfrak{L}_i = \{\ell \in \mathfrak{L} \mid |v \cap \ell| = i\} \qquad \text{for } 0 \le i \le n+1.$$

We have three linear equations in the $|\mathfrak{L}_i|$ which often are linearly independent: First, obviously

$$|\mathfrak{L}_0| + \cdots + |\mathfrak{L}_{n+1}| = |\mathfrak{L}| = n^2+n+1 \tag{1}$$

Secondly, we count incidences in $(\mathfrak{P}\backslash v, \mathfrak{L})$ and obtain

$$(n+1)|\mathfrak{L}_0| + n|\mathfrak{L}_1| + \cdots + 2|\mathfrak{L}_{n-1}| + |\mathfrak{L}_n| = (n+1)\,|\mathfrak{P}\backslash v|. \tag{2}$$

Thirdly, we count the function of the 2-subsets of v into $\mathfrak{L}_2 \cup \cdots \cup \mathfrak{L}_{n+1}$ given by $\{P,Q\} \mapsto PQ$ for $P,Q \in v$ and $P \neq Q$. This leads to

$$\binom{2}{2}|\mathfrak{L}_2| + \binom{3}{2}|\mathfrak{L}_3| + \cdots + \binom{n+1}{2}|\mathfrak{L}_{n+1}| = \binom{|v|}{2}. \tag{3}$$

a) Assume that $|v| = n+3$, and let $\ell \in \mathfrak{L}$. Then $|\ell \cap v| \equiv |v| \equiv 1 \pmod 2$ and $|\ell \cap v| \le 3$ by 3.4 and 3.6. So $\mathfrak{L} = \mathfrak{L}_1 \cup \mathfrak{L}_3$. The equation (3) implies that $|\mathfrak{L}_3| = (n+3)(n+2)/6$. Also, whenever P and Q are two different points in v, then $PQ \in \mathfrak{L}_3$. So $(v, \mathfrak{L}_3)$ is a Steiner triple system.

b) <u>If</u> $|v| = n+4$, <u>then</u> v <u>is a cylinder of hight</u> 4. To prove this we observe that $\mathfrak{L} = \mathfrak{L}_0 \cup \mathfrak{L}_2 \cup \mathfrak{L}_4$, again by 3.4 and 3.6. The equations (1)-(3) imply that $|\mathfrak{L}_0| = (2n^2-5n)/4$, $|\mathfrak{L}_2| = n(n+4)/2$ and $|\mathfrak{L}_4| = (n+4)/4$. Let $P \in v$ and suppose that $[P] \cap \mathfrak{L}_4$ contains 2 different lines ℓ_1 and ℓ_2. Then ℓ_1 and ℓ_2 already contain 7 points of v. Also, each further line in [P] contains at least one further point of v by 3.4. So $|v| > n+4$, a contradiction. Therefore [P] contains at most one line of $\mathfrak{L}_4$,

so that actually $|[P] \cap \mathfrak{L}_4| = 1$, because $|\mathfrak{L}_4| = (n+4)/4$. So v is the union of certain collinear point sets of cardinality 4, which are pairwise disjoint, and each line not intersecting in one of these distinguished point sets intersects v in at most 2 points. This is what we call a cylinder of hight 4.

c) If $|v| = n + 5$, then $n \leq 16$. Because in this case each line intersects v in 1, 3 or 5 points by 3.4 and 3.6. So we have the 3 equations

$$|\mathfrak{L}_1| + |\mathfrak{L}_3| + |\mathfrak{L}_5| = n^2+n+1,$$

$$n|\mathfrak{L}_1| + (n-2)|\mathfrak{L}_3| + (n-4)|\mathfrak{L}_5| = (n^2-4)(n+1), \text{ and}$$

$$\binom{3}{2}|\mathfrak{L}_3| + \binom{5}{2}|\mathfrak{L}_5| = \binom{n+5}{2}.$$

There is exactly one solution: $|\mathfrak{L}_1| = 9n(n-2)/8$, $|\mathfrak{L}_3| = n(16-n)/4$ and $|\mathfrak{L}_5| = (n-2)(n-4)/8$. As $|\mathfrak{L}_3|$ is a non-negative integer, it follows, that $n \leq 16$.

Assume $n = 16$. Then $\mathfrak{L}_3 = \emptyset$ and $|\mathfrak{L}_5| = 21$. Counting incidences in $(v, \mathfrak{L}_5)$ we see that $|[P] \cap \mathfrak{L}_5| = 5$ for $P \in v$. If $\ell \in \mathfrak{L}_5$, then there are $4|\ell \cap v| = 20$ lines different from ℓ in $\mathfrak{L}_5$ which intersect ℓ in v. Therefore v is a Baer subplane.

Assume $n = 4$. Then $\mathfrak{L}_5 = \emptyset$ and $|\mathfrak{L}_3| = 12$. So any two different points P and Q in v are incident with exactly one line in $\mathfrak{L}_3$. Also, $|v| = 2^3+1$, so that $(v, \mathfrak{L}_3)$ is a unital by definition.

If $n = 2$, then $v = \mathfrak{P} = E$.

3.7

There remain 8 and the non-prime powers 6, 10, 12, 14. Here 6 and 14 are excluded by the Bruck-Ryser Theorem. That $n = 10$ is not possible is the main result in MacWilliams, Sloane and Thompson (1973). As far as we know, the case $n = 12$ is still open.

§ 4. On planes of small even order

In this paragraph we mainly want to determine the weight distribution $(w_0, w_1, \cdots)$ of $\mathfrak{A}$ over GF(2) in the cases n = 2 or 4. By 2.3c) it is sufficient to investigate $\mathfrak{A}_{\ddot{o}}$. If n = 2, then dim $\mathfrak{A}_{\ddot{o}} = 3$ by 2.5. Therefore $\mathfrak{A}_{\ddot{o}} = \{E+\ell \mid \ell \in \mathfrak{L}\} \cup \{0\}$, and we obtain $w_0 = w_7 = 1$, $w_3 = w_4 = 7$ and $w_i = 0$ otherwise.

Assume now that n = 4. (The weight enumerator of planes of order 4 has also been previously determined by Asmus (1970) and Erbach (1977)).

4.1 Lemma. Each quadrangle is contained in exactly one hyperoval.

Proof. Let $\mathfrak{x}$ be a quadrangle in $(\mathfrak{P},\mathfrak{L})$. Then the 6 secants of $\mathfrak{x}$ carry 19 points. There remain 2 points P and Q. Let f be the sum of all secants. Then $E + f = \{D_1, D_2, D_3\} \cup \{P,Q\}$, where D_1, D_2 and D_3 are the 3 diagonal points of $\mathfrak{x}$. So $E+f \in \mathfrak{L}$ by 3.7. This shows that $\mathfrak{x} \cup \{P,Q\}$ is a hyperoval (and at the same time that $\mathfrak{x} \cup \{D_1, D_2, D_3\}$ is a subplane).

4.2. $w_9 \geq 280$.

Proof. Let Δ be a triangle in $\mathfrak{P}$ and f the sum over its sides. Then $f \in \mathfrak{A}_9$. In this way we obtain a map of the set of triangles into $\mathfrak{A}_9$. Let Δ' be a second triangle, and assume that the sum f' over its sides equals f. If ℓ is a side of Δ',

then $\ell \cap \Delta = \emptyset$, because $|\ell \cap f| = 3$. So the preimages of f lie in $\mathbb{P}\backslash f$ and are pairwise disjoint. Therefore their number is at most 12/3 = 4, and

$$w_9 \geq (n^2+n+1)(n^2+n)n^2 / 3! \cdot 4 = 280.$$

4.3. $w_8 \geq 210$.

Proof. If $\ell_1, \ell_2 \in \Omega$ and $\ell_1 \neq \ell_2$, then $|\ell_1+\ell_2| = 8$. The representation of $\ell_1 + \ell_2$ as sum of 2 lines is unique (up to ordering), because any line different from ℓ_1 and ℓ_2 intersects $\ell_1 + \ell_2$ at most in 2 points. So $w_8 \geq \binom{21}{2}$. (Actually, $w_8 = \binom{21}{2}$ by 3.10b)).

Now $\overline{\mathfrak{A}} \leq \overline{\mathfrak{A}}^\perp$ by 2.4, and actually $\overline{\mathfrak{A}} < \overline{\mathfrak{A}}^\perp$ by 4.1 and 3.8. So dim $\overline{\mathfrak{A}} \leq 10$, and dim $\mathfrak{A}_{\ddot{o}} \leq 9$. On the other hand, $\mathfrak{A}_{\ddot{o}}$ contains 0, 21 complements of lines, $\binom{21}{2} = 210$ sums of two different lines and at least 280 vectors of weight 12 by 4.2. Therefore dim $\mathfrak{A} = 10$, $w_0 = w_{21} = 1$, $w_5 = w_{16} = 21$, $w_8 = w_{13} = 210$ and $w_9 = w_{12} = 280$, while all other coefficients are trivial.

We collect some further information about $(\mathbb{P},\Omega)$:

4.4 Lemma. The number of hyperovals is 168.

Proof. 4.1 provides us with a map of the set of quadrangles into the set of hyperovals. The number of preimages for each hyperoval is $\binom{6}{4} = 15$. Thus the number of hyperovals is $21 \cdot 20 \cdot 16 \cdot 9 / 4! \cdot 15 = 168$.

By 2.3c), $\mathfrak{P}^* = \overline{E} \in \overline{\mathfrak{U}}$. If $v \in \overline{\mathfrak{U}}^\perp \setminus \overline{\mathfrak{U}}$, then $0 = (v,\mathfrak{P}^*) = (v,v)$, so that $\overline{\mathfrak{U}} + \langle v \rangle$ is self-orthogonal. Hence $\overline{\mathfrak{U}}^\perp$ contains 3 self-orthogonal subspaces containing $\overline{\mathfrak{U}}$, say $\mathfrak{S}$, $\mathfrak{S}'$ and $\mathfrak{S}''$.

We now assume that $(\mathfrak{P},\mathfrak{L}) = PG(2,4)$. Then $P\Gamma L(3,4)$ acts on $\mathfrak{P}$. We extend this action to $\mathfrak{P}^*$ by letting the group act trivially on $\{P_0\}$. Clearly $P\Gamma L(3,4)$ leaves invariant $\overline{\mathfrak{U}}$, and $PSL(3,4)$ lies in the kernel of the action of $P\Gamma L(3,4)$ on $\overline{\mathfrak{U}}^\perp / \overline{\mathfrak{U}}$. Let R be a group of order 3 of homologies in $PGL(3,4)$. R has 5 nontrivial orbits in $\mathfrak{P}^*$. Hence the module (V^*,R) has 5 non-trivial composition factors. But $(V^* / \overline{\mathfrak{U}}^\perp,R)$ is contragredient to $(\overline{\mathfrak{U}},R)$. So these two modules together have an even number of non-trivial composition factors. This implies that R is non-trivial on $\overline{\mathfrak{U}}^\perp / \overline{\mathfrak{U}}$ [1]. As $P\Gamma L(3,4) / PSL(3,4) \cong S_3$, we obtain

4.5. $P\Gamma L(3,4)$ is 2-transitive on $\{\mathfrak{S},\mathfrak{S}',\mathfrak{S}''\}$.

Let $\mathfrak{L}^* = \mathfrak{S}_6$ and $\mathfrak{H}$ the set of hyperovals in $\mathfrak{S}$. Then $\mathfrak{L}^* = \overline{\mathfrak{U}} \cup \mathfrak{H}$ by 3.7 and 3.8.

4.6. $|x \cap y| = 0$ or 2 for $x,y \in \mathfrak{L}^*$ and $x \neq y$.

Proof. This is trivial if $x \in \overline{\mathfrak{U}}$. Assume that $x,y \in \mathfrak{H}$. Then $x,y \in \mathfrak{S} \setminus \overline{\mathfrak{U}}$ by 3.8 and hence $x+y \in \overline{\mathfrak{U}}$, so that $|x+y| \geq 5$. On the other hand, $2 \mid |x \cap y|$, because $\mathfrak{S}$ is self-orthogonal.

---

[1]) This argument I owe to Hans-Jörg Schaeffer. The statement also follows from 6.1b').

The Mathieu group M_{22}

The symmetric group $S^{\mathcal{P}^*}$ acts on V^*. We define $\tilde{M}_{22}$ to be the stabilizer of $S^{\mathcal{P}^*}$ on $\mathfrak{S}$. By 3.7 the stabilizer of $\tilde{M}_{22}$ on P_0 leaves invariant $\mathcal{Q}$. Therefore it is faithfully represented on the projective plane $(\mathcal{P},\mathcal{Q})$, so that this stabilizer is a subgroup of $P\Gamma L(3,4)$ containing $PSL(3,4)$ as a subgroup of index 2 by 4.5. In particular, $(\tilde{M}_{22})_{P_0}$ is 2-transitive on $\mathcal{P}$, and $|\tilde{M}_{22}| \leq 22 \cdot 2 \cdot |PSL(3,4)|$.

4.7. *$\tilde{M}_{22}$ is triply transitive on $\mathcal{P}^*$, and $|\tilde{M}_{22}| = 22 \cdot 2 \cdot |PSL(3,4)|$.*

Proof. We only have to show that $\tilde{M}_{22}$ contains an element moving P_0. Let $Q \in \mathcal{P}$, $\mathcal{Q}' = \{b \in \mathcal{Q}^* \mid Q \in b\}$ and consider the incidence geometry

$$\mathfrak{x} = \left(\mathcal{P}^* - \{Q\},\ \{b-\{Q\} \mid b \in \mathcal{Q}'\}\right).$$

$|\mathfrak{G}| = 56$ by 3.8, 4.4 and 4.5. Counting incidences in $(\mathcal{P},\mathfrak{G})$, we obtain $|\mathcal{P}|u = |\mathfrak{G}|6$, where u is the number of hyperovals in $\mathfrak{G}$ containing Q. Hence $u = 16$, and $|\mathcal{Q}'| = 21$. Now 4.6 implies that $\mathfrak{x}$ is a projective plane of order 4. Hence $\mathfrak{x} \cong (\mathcal{T},\mathcal{Q})$ by Witt (1938). Therefore there exists a bijection φ of $\mathcal{P}^* - \{Q\}$ onto $\mathcal{P}$ which maps $\{\ell-\{Q\} \mid \ell \in \mathcal{Q}'\}$ onto $\mathcal{Q}$. We extend φ to a permutation of $\mathcal{P}^*$ by defining $Q^\varphi = P_0$. Note that φ maps $\mathcal{Q}'$ onto $\overline{\mathcal{U}}$, and hence $\langle\mathcal{Q}'\rangle$ onto $\langle\overline{\mathcal{U}}\rangle = \overline{\mathcal{U}}$. Here $\mathfrak{S} \perp \langle\mathcal{Q}'\rangle$, as $\mathfrak{S}$ is self-orthogonal, and therefore $\mathfrak{S}^\varphi \perp \langle\mathcal{Q}'\rangle^\varphi = \overline{\mathcal{U}}$. Hence $\mathfrak{S}^\varphi \in \{\mathfrak{S},\mathfrak{S}',\mathfrak{S}''\}$, and by 4.5 there exists $\xi \in P\Gamma L(3,4)$ such that $\mathfrak{S}^{\varphi\xi} = \mathfrak{S}$. Now $\varphi\xi \in \tilde{M}_{22}$ and $Q^{\varphi\xi} = P_0$.

§ 5. Some remarks on group spaces

Let (Ω,G) be a finite group space, F a field and V the set of functions of Ω into F. Together with pointwise addition and the obvious multiplication, V is a vector space over F. For $f \in V$ and $g \in G$ we define a function $f^g \in V$ by

$$f^g(\alpha) = f(\alpha^{g^{-1}}) \qquad \text{for all } \alpha \in \Omega.$$

With this binary operation V is a FG-module. This is the permutation module over F of the group space (Ω,G). Our group G leaves invariant bilinear forms on V: Let $\Omega_1,\cdots,\Omega_t$ be the orbits of G in Ω and $a_1,\cdots,a_t \in F$. Define

$$(f,g) = a_1 \sum_{x\in\Omega_1} f(x)g(x) + a_2 \sum_{x\in\Omega_2} f(x)g(x)+\cdots+ a_t \sum_{x\in\Omega_t} f(x)g(x).$$

Then $(\ ,\ )$ is a bilinear form invariant under G. Note that $(\ ,\ )$ is non-degenerate if and only if $a_1,\cdots,a_t \neq 0$.

In the following we investigate the situation that $a_1,\cdots,a_t \neq 0$ and G leaves invariant a subspace M of V such that $M = M^{\perp}$ ($^{\perp}$ with respect to $(\ ,\ )$). Note that dim V is necessarily even, and dim $M = \frac{1}{2}$ dim V.

5.1 Lemma. Let $A_1,\cdots,A_s$ be the factors of a composition series of the G-module V. Then there exists a fixed-point-free involutory permutation α of $\{A_1,\cdots,A_s\}$ such that A_i^{α} is the contragredient module of A_i for $1 \leq i \leq s$.

Proof. Let

$$0 = M_0 < M_1 < \cdots < M_n = M$$

be a composition series of M. Then

$$0 = M_0 < M_1 < \cdots < M_n < M_{n-1}^{\perp} < \cdots < M_1^{\perp} < M_0^{\perp} = V$$

is a composition series of V. Here the G-module $M_i^{\perp} / M_{i+1}^{\perp}$ is contragredient to M_{i+1} / M_i for $0 \leq i \leq n-1$. So the map α interchanging M_{i+1} / M_i and $M_i^{\perp} / M_{i+1}^{\perp}$ for $0 \leq i \leq n-1$ has the required properties.

5.2 Lemma. Assume that char F $\nmid$ |G|. Then $\dim \mathfrak{C}_M G = \frac{1}{2} \dim \mathfrak{C}_V G$ and $\dim [M,G] = \frac{1}{2} \dim [V,G]$.

Proof. Since G is completely reducible, $\dim \mathfrak{C}_V G$ is equal to the number of trivial composition factors of (V,G). So by 5.1 the number of trivial composition factors of (M,G) is $\frac{1}{2} \dim \mathfrak{C}_V G$, and the first equality of our lemma follows. The second equality follows from the fact that $V = [V,G] \oplus \mathfrak{C}_V G$. This implies $\dim [M,G] = \dim M - \dim \mathfrak{C}_M G = \frac{1}{2} \dim V - \frac{1}{2} \dim \mathfrak{C}_V G = \frac{1}{2} \dim [V,G]$.

A second proof for Lemma 5.2 can be established with the help of the following fact:

5.3 Lemma. $[V,G] \perp \mathfrak{C}_V G$. If G is cyclic or char F $\nmid$ |G|, then $[V,G] = (\mathfrak{C}_V G)^{\perp}$.

Proof. Let $v \in V$, $g \in G$ and $w \in \mathfrak{C}_V G$. Then

$$([v,g],w) = (vg-v,w) = (vg,w)-(v,w) = (vg,wg)-(v,w) = 0.$$

Hence $[V,G] \leq (\mathfrak{C}_V G)^\perp$. If $G = \langle g \rangle$, then $[V,G] \geq V(g-1)$ so that $\dim [V,G] \geq \dim V(g-1) = \dim V - \dim \mathfrak{C}_V G = \dim (\mathfrak{C}_V G)^\perp$. If $\mathrm{char}\ F \nmid |G|$, then $V = [V,G] \oplus \mathfrak{C}_V G$, so that again $\dim [V,G] = \dim (\mathfrak{C}_V G)^\perp$.

So if $\mathrm{char}\ F \nmid |G|$, then V is an orthogonal direct sum of $[V,G]$ and $\mathfrak{C}_V G$. Therefore $(\ ,\ )$ induces a non-degenerate bilinear form on these spaces, and hence $\dim (M \cap [V,G]) \leq \frac{1}{2} \dim [V,G]$ and $\dim (M \cap \mathfrak{C}_V G) \leq \frac{1}{2} \dim \mathfrak{C}_V G$, as $M \leq M^\perp$. On the other hand, $M = [M,G] \oplus \mathfrak{C}_M G$, $[M,G] \leq M \cap [V,G]$, $\mathfrak{C}_M G \leq M \cap \mathfrak{C}_V G$ and $\dim M = \frac{1}{2} \dim V$. This implies 5.2.

5.4 Corollary. Assume that F has finite characteristic p and that G has prime order $r \neq p$. If the number of non-trivial orbits of G in Ω is odd, then $r > 2$ and $r \mid p^{(r-1)/2}-1$.

Proof. Let m be the number of non-trivial orbits of G in Ω. Then the total number of orbits of G is $m+|\Omega| - mr$. So $\dim \mathfrak{C}_M G = \frac{1}{2} \dim \mathfrak{C}_V G = \frac{1}{2} (m+|\Omega| - rm)$ and hence $\dim M/\mathfrak{C}_M G = (|\Omega|-m-|\Omega|+rm)/2 = m(r-1)/2$ by 5.2. Now G acts frobeniusly on $M/\mathfrak{C}_M G$, so that $r \mid p^{m(r-1)/2} - 1$. Let e be the order of p in $\mathbb{Z} / r\mathbb{Z}$. Then $e \mid m(r-1)/2$. On the other hand, $e \mid (r-1)$ by Fermat's Theorem. So $e \mid (m(r-1)/2, r-1) = (r-1)/2$ as $m \equiv 1 \pmod 2$.

Note that the condition $r \mid p^{(r-1)/2} - 1$ is equivalent to the property that p is a square in $\mathbb{Z} / r\mathbb{Z}$, i.e. p is a quadratic

residue modulo r. Corollary 5.4 also is a corollary of the Theorem 5.5 below.

5.5 Theorem. Assume that G is cyclic of order n and that F has finite characteristic p such that $p \nmid n$. If the number of orbits of length n of G is odd, then $n > 2$ and $n \mid p^{\varphi(n)/2} - 1$.

Proof. We count the faithful composition factors of the G-module (V,G): For $1 \leq i \leq t$ we define

$$V(\Omega_i) = \{f \in V \mid f(\xi) = 0 \text{ for all } \xi \in \Omega - \Omega_i\}.$$

Then

$$V = V(\Omega_1) \perp \cdots \perp V(\Omega_t),$$

and $V(\Omega_i)$ is a G-submodule for $1 \leq i \leq t$. If $|\Omega_i| = |G|$, then the number of faithful composition factors of $(V(\Omega_i),G)$ is $\varphi(n)/e$, where e is the order of p in the group of units of $\mathbb{Z}/n\mathbb{Z}$. If, on the other hand, $|\Omega_i| < |G|$, then $V(\Omega_i)$ does not have any faithful composition factor at all. To prove this, choose any element $\alpha \in \Omega_i$. Then $G_\alpha \neq 1$, and $\Omega_i = \alpha^G \subseteq \Omega(G_\alpha)$, as G is abelian. Therefore G_α actually is trivial on $V(\Omega_i)$. So the number of non-trivial composition factors of (V,G) in $\overline{t}\varphi(n)/e$, where $\overline{t}$ is the number of regular orbits of G in Ω. So $\overline{t}\varphi(n)/e$ is even by 5.1. As $\overline{t}$ is odd by our assumption, it follows that $2 \mid \varphi(n)/e$. In particular $n > 2$.

We present a further simple example of an application of 5.1, which will be useful for our investigations of

collineation groups of projective planes:

5.6 Lemma. Assume that F has finite characteristic $p \neq 3$ and that G is a 3-group. Assume furthermore, that $|\Omega_1| = 1$, $|\Omega_2| = 3$ and $|\Omega_i| = |G|$ for $3 \leq i \leq t$. Then $3 \mid p-1$.

Proof. As above, we have the orthogonal direct decomposition

$$V = V(\Omega_1) \perp V(\Omega_2) \perp \cdots \perp V(\Omega_t).$$

Suppose that $3 \nmid p-1$. Then $V(\Omega_2) = V_{21} \oplus V_{22}$, where V_{21} and V_{22} are irreducible G-submodules such that V_{21} is trivial and $\dim V_{22} = 2$. We count the number of composition factors of (V,G) of dimension 2: $V(\Omega_2)$ contains one, and therefore the total number is odd, as $t-2 = (|\Omega|-4) / |G| \equiv |\Omega|-4 \equiv |\Omega| \equiv 0 \pmod 2$. So we obtain a contradiction to 5.1.

5.7 Lemma. a) If char F $\nmid |G|$, then the number of orbits of G in Ω is even.
b) If char F $\neq 2$, then each element in G induces an even permutation of Ω.

Proof. a) $t = \dim \mathfrak{C}_V G$. If char F $\nmid |G|$, then $\dim \mathfrak{C}_V G$ is the number of trivial composition factors of (V,G), and this number is even by 5.1.

b) Assume that char F $\neq 2$, and let x be a 2-element in G. Then $|\Omega(x)| \equiv |\Omega| \equiv 0 \pmod 2$. So the number of trivial orbits of $\langle x \rangle$ in Ω is even, and by a) the number of non-

trivial orbits is even likewise. Let $\Omega_1, \cdots, \Omega_u$ be these latter orbits. Then x can be written as the product of $(|\Omega_1|-1) + \cdots + (|\Omega_u|-1)$ transpositions. This number is congruent to u and hence to 0 modulo 2.

§ 6. Collineation groups represented on codes

We now return to our projective planes: Let $(\mathfrak{P},\mathfrak{L})$ be a projective plane of finite order n and F a field of finite characteristic p. Let $V,\mathfrak{L},P_0,\mathfrak{P}^*,V^*$, the bilinear form $(\ ,\ )$ and the homomorphism - be defined as in § 2. In addition, let G be a group of automorphisms of $(\mathfrak{P},\mathfrak{L})$. From the group space $(\mathfrak{P},G)$ we obtain a group space $(\mathfrak{P}^*,G)$ by defining

$$P_0{}^g = P_0 \qquad \text{for all } g \in G.$$

As in § 5 we make V^* to a G-module. Note that for $\ell \in \mathfrak{L}$ and $g \in G$

$$\left(\overline{f_{(\ell)}}\right)^g = \overline{f_{(\ell^g)}}\ .$$

In particular, G leaves invariant $\overline{\mathfrak{L}}$. If $p \mid n$ but $p^2 \nmid n$, then $\overline{\mathfrak{L}}$ is self orthogonal, and we can apply the techniques and results of § 5. As an immediate consequence we have:

6.1 Theorem. Let $(\mathfrak{P},\mathfrak{L})$ be a projective plane of finite order n and G a group of automorphisms of $(\mathfrak{P},\mathfrak{L})$. Assume that there exists a prime p such that $p \mid n$ but $p^2 \nmid n$. Then

a) Assume that G is cyclic of order m and that $p \nmid m$. If the number of orbits of length m of G is odd, then $m > 2$ and $m \mid p^{\varphi(m)/2} - 1$.

b) Assume that G has prime order $r \neq p$. If $|\mathfrak{P}(G)|$ is even, then $r > 2$ and $r \mid p^{(r-1)/2} - 1$.

c) Assume that $2 \nmid n$ and that G contains an elation of prime order $r \neq p$. Then $r \mid p^{(r-1)/2} - 1$.

d) Assume that $2 \mid n$ and that G contains a homology of prime order $r \neq p$. Then $r \mid p^{(r-1)/2} - 1$.

e) Assume that $p \neq 3$ and that G is a 3-group fixing a subset $\mathfrak{x}$ of cardinality 3 of $\mathfrak{P}$. If G is semi-regular on $\mathfrak{P}-\mathfrak{x}$, then $\mathfrak{x} \subseteq \mathfrak{P}(G)$ or $3 \mid p-1$.

f) If $p \nmid |G|$, then the number of orbits of G in $\mathfrak{P}$ is odd.

Proof. We use 5.4 - 5.7. To prove b) note that $|\mathfrak{P}| = n^2+n+1 \equiv 1 \pmod 2$, so that the number of non-trivial orbits of G is odd, if G has prime order and $|\mathfrak{P}(G)|$ is even. b) implies c) and d), as in these cases the number of non-trivial orbits of G is n^2/r and $(n^2-1)/r$ respectively.

b) and f) in Theorem 6.1 can be deduced from Theorem 3.1 in Hughes (1957).

If $p^2 \mid n$, then the same technique still provides some information about the action of G on $\mathfrak{x}^\perp / \mathfrak{x}$. Actually, we can generalize and rephrase all our results in this way. For example we have

6.1b'). Let $(\mathfrak{P},\mathfrak{L})$ be a projective plane of finite order n, and G a group of automorphisms of $(\mathfrak{P},\mathfrak{L})$. Assume that F has finite characteristic p such that $p \mid n$. If G has prime order $r \neq p$ and $|\mathfrak{P}(G)| \equiv 0 \pmod 2$, then $r > 2$ and $r \mid p^{(r-1)/2} - 1$ or G acts non-trivially on $\mathfrak{x}^\perp / \mathfrak{x}$.

§ 8. Generalization to projective designs

Let $(\mathcal{P},\mathcal{B})$ be an incidence structure such that there exist $\lambda,k \in \mathbb{N}$ with the properties

a) $|(b)| = k$ for all $b \in \mathcal{B}$,

b) $|(b) \cap (c)| = \lambda$ for all $b,c \in \mathcal{P}$ such that $b \neq c$,

c) $|\mathcal{P}| = |\mathcal{B}|$, and

d) $\lambda < k < |\mathcal{P}| - 1$.

Denote $v = |\mathcal{P}|$ and $n = k-\lambda$. We call $(\mathcal{P},\mathcal{B})$ a <u>projective design</u> and n the <u>order</u> of $(\mathcal{P},\mathcal{B})$. Let A be the incidence matrix of $(\mathcal{P},\mathcal{B})$. We see that $AA^t = nI + \lambda J$, where I is the $v \times v$ identity matrix and J is the $v \times v$-matrix all of whose entries are 1. It follows that $A^tA = AA^t$ (see Ryser, 1963, Theorem 2.1). Therefore $|[P]| = k$ for all $P \in \mathcal{P}$ and $|[P] \cap [Q]| = \lambda$ for all $P,Q \in \mathcal{P}$ such that $P \neq Q$. Counting incidences we obtain $k(k-1) = (v-1)\lambda$ and hence $v = (n+\lambda)(n+\lambda-1)/\lambda+1$. Also, $(\det A)^2 = \det (nI+\lambda J) = (n+\lambda)^2 n^{v-1}$. Hence $|\det A| = (n+\lambda)n^{(v-1)/2}$ and in particular v is odd or n is a square (Schützenberger, 1949).

We now proceed in a way very similar to that of § 2. However we want to apply a slightly different method for the determination of the dimensions of the codes generated by $(\mathcal{P},\mathcal{B})$, which is much more clear from the geometric point of view. This makes it necessary to replace sometimes the ground field F by the ring $\mathbb{Z}$ of rational intergers. So we generalize our concept a little.

Let R be any ring with 1 and V the set of functions from $\mathfrak{P}$ into R. Then V is a free R-module. As $1 \in R$ we can define characteristic functions as before. Let $\mathfrak{A}$ be the R-submodule generated by the set

$$\{f_{(b)} \mid b \in \mathfrak{B}\}.$$

The element E we define as in § 2.

We consider at first the case $R = \mathbb{Z}$. Then $\mathfrak{A}$ is a sublattice of the complete lattice V, and we can easily obtain a lot of information about the factor group $V/\mathfrak{A}$. We already know

8.1 Lemma. The abelian group $V/\mathfrak{A}$ is finite of order $|\det A| = (n+\lambda)n^{(v-1)/2}$.

8.2 Lemma. Assume that $R = \mathbb{Z}$. Let d be the order of $E + \mathfrak{A}$ in $V/\mathfrak{A}$, and let p be a prime. Then

a) $d \mid n+\lambda$,

b) if $p^c \parallel n+\lambda$, then $p^c \mid d$, unless $p|v$, $p^c|n$ and $p^c \parallel \lambda$; and

c) if $(n,\lambda) = 1$, then $d = n+\lambda$.

Proof. a) Let

$$f = \sum_{b \in \mathfrak{B}} f_{(b)}$$

and $X \in \mathfrak{P}$. As $f_{(b)}(X) = 1$ if $X \in (b)$ and $f_{(b)}(X) = 0$ otherwise, we have $f(X) = |[X]| = n+\lambda$ and hence

$$\sum_{b \in \mathfrak{B}} f_{(b)} = (n+\lambda)\, E.$$

In particular $(n+\lambda)\, E \in \mathfrak{A}$, so that $d \mid n+\lambda$.

b) We can assume that $c > 0$. Define

$$V_{n+\lambda} = \{f \in V \mid n+\lambda \Big| \int_{\mathfrak{P}} f\}.$$

Clearly, $V_{n+\lambda}$ is a subgroup of V, and $\mathfrak{A} \leq V_{n+\lambda}$. As $d\,E \in \mathfrak{A} \leq V_{n+\lambda}$, $p^c \Big| n+\lambda \Big| \int_{\mathfrak{P}} dE = dv$. Suppose now, that $p^c \nmid d$. Then $p \mid v = (n+\lambda)(n+\lambda-1)/\lambda+1$. Thus $p \nmid (n+\lambda)(n+\lambda-1)/\lambda$, and hence $p^c \mid \lambda$, as $p^c \mid n+\lambda$ by hypothesis. So $p^c \mid n$. Suppose that $p^{c+1} \mid \lambda$. As $c > 0$, $p \mid n+\lambda$, and as $\lambda \mid (n+\lambda)(n+\lambda-1)$ we obtain $p^{c+1} \mid n+\lambda$, contradicting our hypothesis. So $p^c \parallel \lambda$.

c) follows immediately from b).

8.3 Lemma. Assume that $R = \mathbb{Z}$. The exponent of $V/\mathfrak{A}$ divides $(n+\lambda)n$.

Proof. This follows from the fact, that for each point $P \in \mathfrak{P}$ the sublattice $\mathfrak{A}$ contains the element

$$(n+\lambda) \sum_{b \in [P]}{}' f_{(b)} - \lambda(n+\lambda)E = n(n+\lambda)f_{\{P\}}.$$

We now have quite some information about Sylow-p-subgroups of $V/\mathfrak{A}$, in particular, if p is a prime dividing n to the first power: Let p be a prime such that $p \parallel n$. If $p \nmid \lambda$, then $p \nmid n+\lambda$, so that S is just an elementary abelian group of order $p^{(v-1)/2}$ by 8.1 and 8.3. If $p \mid \lambda$ and p^c is the highest power of p dividing $n+\lambda$, then S contains a cyclic subgroup of order p^c by 8.2 (In fact, $\langle E+\mathfrak{A} \rangle$ contains a cyclic group of order p^c unless c=1). On the other hand, in this case $|S| \Big| p^{c+(v-1)/2}$.

So we have

8.4 Lemma. Let p be a prime such that $p \mid n$ but $p^2 \nmid n$, and let S be a Sylow p-subgroup of $V/\mathfrak{A}$.
a) If $p \nmid \lambda$, then the rank of S is $(V-1)/2$.
b) If $p \mid \lambda$, then the rank of S is at most $(v-1)/2 +1$.

This is very important here because of the following fact:

8.5 Lemma. Let p be any prime and S a Sylow p-subgroup of $V/\mathfrak{A}$. Denote the rank of S by u. Then $|\mathfrak{P}|-u$ is the dimension of the code $\mathfrak{A}_p$ of $(\mathfrak{P},\mathfrak{B})$ over GF(p).

Proof. $V/(pV+\mathfrak{A}) \cong V/\mathfrak{A} \,/\, (pV+\mathfrak{A})/\mathfrak{A}$. Here $(pV+\mathfrak{A})/\mathfrak{A} = p(V/\mathfrak{A})$, so that $V/(pV+\mathfrak{A}) \cong V/\mathfrak{A} \,/\, p(V/\mathfrak{A})$. This is an elementary abelian p-group of order p^u.

We now assume that R is a field of characteristic p. We have to distinguish four cases:

8.6. If $p = \infty$ or $p < \infty$ but $p \nmid (n+\lambda)n$, then $\mathfrak{A} = V$, because $|\det A| = (n+\lambda)n^{(v-1)/2}$.

8.7. If $p < \infty$, $p \mid (n+\lambda)$ but $p \nmid n$, then $\mathfrak{A}$ is a hyperplane of V by 8.1, 8.2 and 8.5.

8.8. Assume that $p < \infty$, $p \mid n$ but $p \nmid n+\lambda$. To obtain further information, we proceed like in § 2: We augment $\mathfrak{P}$ by a new point P_0 to a set $\mathfrak{P}^* = \{P_0\} \cup \mathfrak{P}$ and denote $V^* = R^{\mathfrak{P}^*}$.

For $f \in V$ we define $\overline{f} \in V^*$ by

$$\overline{f}(P_0) = -\int_{\mathfrak{P}} f \text{ and}$$

$$\overline{f}(X) = f(X) \qquad \text{for all } X \in \mathfrak{P}.$$

Also, we define a bilinear form $(\ , \ )$ on V^*:

$$(f,g) = -f(P_0)g(P_0) + \lambda \int_{\mathfrak{P}} fg \qquad \text{for all } f,g \in V^*.$$

Here fg stands for the pointwise product of f and g. As $p \nmid \lambda$, this form is non-degenerate. One easily sees, that $\overline{\mathfrak{A}} \leq \overline{\mathfrak{A}}^{\perp}$, so that $\dim \mathfrak{A} \leq (V+1)/2$. If $p \parallel n$, then $\dim \mathfrak{A} = v - (v-1)/2 = (v+1)/2$ by 8.4 and 8.5. We summarise:

If $p \parallel n$ *and* $p \nmid \lambda$, *then* $\overline{\mathfrak{A}} = \overline{\mathfrak{A}}^{\perp}$ *and* $\dim \mathfrak{A} = (v+1)/2$.

8.9. Assume that $p < \infty$, $p \mid n$ and $p \mid \lambda$. This case is in some way easier to handle than the previous one: We define $(\ , \ )$ to be just the standard bilinear form on V:

$$(f,g) = \int_{\mathfrak{P}} fg \qquad \text{for all } f,g \in V.$$

Then $\mathfrak{A} \leq \mathfrak{A}^{\perp}$ and $\dim \mathfrak{A} \leq v/2$, as $p \mid \lambda$. Assume now that $p \parallel n$. Then v is odd as pointed out at the beginning of this paragraph. Hence $\dim \mathfrak{A} = V - [(V-1)/2+1] = (V-1)/2$ by 8.4. Note that $\dim \mathfrak{A}^{\perp}/\mathfrak{A} = 1$. Clearly, $\mathfrak{A}$ is contained in the subspace

$$V_{\ddot{o}} = \{f \in V \mid \int_{\mathfrak{P}} f = 0\}.$$

So $E \notin \mathfrak{A}$ unless $p \mid v$. We summarise:

If $p \parallel n$ *and* $p \mid \lambda$, *then* $\mathfrak{A} \leq \mathfrak{A}^{\perp}$ *and* $\dim \mathfrak{A}^{\perp}/\mathfrak{A} = 1$, *where* $\mathfrak{A}^{\perp}$ *is the space orthogonal to* $\mathfrak{A}$ *with respect to the ordinary*

scalar product on V. Also, in this case $\mathfrak{A}^{\perp} = \langle E \rangle \oplus \mathfrak{A}$ unless, possibly, if $p \mid v$.

8.8 and 8.9 shows that the techniques of § 5 are applicable to collineation groups of $(\mathfrak{P},\mathfrak{B})$ whenever $p \parallel n$.

References

Asmus, E. Jr.: Algebraic theory of codes II.
A.F.C. Research Laboratories Report 1970.

Erbach, D.W.: The code associated with the projective plane of order four.
Arch. Math. 28 (1977) 669-672.

Hughes, D.R.: Collineations and generalized incidence matrices.
Transactions Amer. Math. Soc. 86 (1957) 284-296.

Lüneburg, H.: Transitive Erweiterungen endlicher Permutationsgruppen.
Berlin, Heidelberg, New York 1969

MacWilliams, F.J., N.J.A. Sloane and J.G. Thompson: On the existence of a projective plane of order 10.
J. of Combinatorial Theory 14 (1973) 66-78

Ryser, H.J.: Combinatorial mathematics.
New Jersey 1963

van der Waerden, B.L.: Algebra.
New Jersey 1963

Witt, E.: Über Steinersche Systeme.
Abh. Math. Sem. Univ. Hamburg 12 (1938) 265-275